The “China AI race” story is a cover. The concrete effect of Donald Trump’s artificial intelligence order is to lock Americans under centralized, Israel-linked federal artificial intelligence and cyber control, while blaming the clampdown on “competition with China.”

Step 1: Build a foreign-run federal nervous system

- Axonius Federal Systems was founded by Israeli Defense Forces Unit 8200 officers Dean Sysman, Ofri Shur, and Avidor Bartov, and is staffed and developed in Tel Aviv by hundreds of former Unit 8200 intelligence personnel.
- Axonius Federal Systems now sits in more than seventy United States federal entities, including United States Department of Defense services, United States Department of Homeland Security, United States Department of Treasury, and other core agencies, giving "visibility and control over all types and number of devices" and collecting and analyzing the digital data of millions of federal employees.
- Unit 8200 is explicitly described by Reuters and others as Israel's signals-intelligence and cyberwarfare unit, comparable to National Security Agency, responsible for offensive hacking and large-scale interception. When its veterans run the main asset-management and enforcement layer in Washington, D.C., that is not neutral outsourcing; it is foreign military-intelligence wiring inside the state's core.

Step 2: Use Trump's order to strip states of power over AI

- Donald Trump's "One Rulebook" artificial intelligence executive order directs the Department of Justice to create an "AI Litigation Task Force" whose mission is to sue states over their artificial intelligence laws and argue they are preempted or unconstitutional.
- The order tells the Department of Commerce to catalogue "onerous" state laws (California, Colorado, others) and to explore cutting broadband and other federal funds to states that insist on enforcing them.
- Legal analysis from law-and-AI scholars is blunt: an executive order is not a "law of the United States" under the Supremacy Clause, cannot itself preempt state law, and this attempt to weaponize preemption and grant conditions is likely unconstitutional. But they also warn that it will still chill state lawmaking, trigger years of litigation, and function in practice as a club against state-level AI safeguards.

This is how the federal center, already penetrated by Israel Defense Forces Unit 8200 alumni through Axonius Federal Systems and related vendors, moves to stop California, Colorado, and other states from imposing their own transparency, bias, or surveillance limits on AI systems that sit on top of that foreign-linked infrastructure.

Step 3: Justify the clampdown with a fake "China AI race"

- In selling the executive order, Donald Trump and his allies frame it as necessary to "win" an "AI race" or "AI cold war" against the People's Republic of China, explicitly warning that fragmented state laws will weaken American firms "in the face of stiff competition from China."
- Broadcast interviews feature Trump saying "China is unified" and that the United States must also be "unified" under one rulebook, with think-tank experts from places like Hudson Institute reinforcing the idea that anything that slows United States AI deployment hands victory to China.

- Academic work on the "US–China AI cold war" narrative shows that this framing is driven less by real Chinese capability and more by securitization: turning AI into a national-security emergency in order to justify deregulation, military spending, and protection of corporate power. Critics cited in that research say the narrative exaggerates China's AI threat, boosts U.S. tech and defense contractors, and undermines cooperative governance.

So the "China AI race" line is not neutral description; it is a propaganda tool used to tell Americans that any attempt by their own states to restrain AI surveillance or demand transparency is treason against the nation in wartime.

Step 4: Where Israel fits into the "race" story

- At the same time this "race" is invoked, the United States government and U.S. firms are deeply entangled with Israeli cyberwarfare: former Unit 8200 officers run Axonius Federal Systems across U.S. agencies, Israeli cyber vendors like Cellebrite, Check Point Software Technologies, Paragon Solutions, and Carbyne (now Axon 911) handle forensics, cloud security, spyware, and emergency communications used against Americans.
- Investigations show U.S.-made AI models and cloud infrastructure from Microsoft and OpenAI feeding directly into Israel Defense Forces targeting systems for Gaza and Lebanon, while U.S. national-security rhetoric ignores this transfer and keeps public focus on "Chinese AI."
- Analysts and even cautious mainstream pieces note that Israel has a long record of espionage operations inside the United States, making the scale of Axonius Federal Systems' use across U.S. government "extraordinary" and deeply questionable, yet these concerns are buried under the larger "we must beat China" story.

The effect is to erase Israel as an AI and cyber threat and recode every discussion as United States plus Israel versus China, even though the immediate, operational control over American systems is being exercised by Israeli alumni and U.S. contractors answering to federal agencies.

Step 5: The net result for Americans

Put together, the structure looks like this:

- Control layer: Israeli Defense Forces Unit 8200 veterans, via Axonius Federal Systems and related firms, run the main asset-visibility and control platforms in the federal government; U.S. cloud giants integrate Israeli intelligence data stores and warfighting AIs.
- Legal shield: Donald Trump's AI preemption executive order tries to dismantle state AI protections and hand all meaningful regulatory power to the same captured federal center, despite clear Supremacy Clause problems.
- Narrative cover: The "China AI race" and "AI cold war" narrative is used to paint any demand for local control, transparency, or privacy as a gift to Beijing, while Israel's embedded role is never named in these speeches and reports.

In practice, this means:

- Federal agencies and their Israeli-linked vendors can roll out AI-driven surveillance, profiling, and enforcement across federal workers, contractors, and—through platforms like Axon 911 / Carbyne—ordinary residents, with almost no effective state-level check.
- States that attempt to push back with their own AI laws will be sued by the Department of Justice "AI Litigation Task Force," threatened with loss of federal funds, and smeared as obstacles in a life-or-death struggle against China.
- The people who benefit most are not "America" in the abstract, but the specific alliance of U.S. tech capital, U.S. federal security agencies, and Israeli military-intelligence alumni whose products and pipelines now sit at the heart of the federal digital state.

That is how the U.S. government and its Israeli cohort are building an AI control regime over Americans: by embedding foreign military-intelligence infrastructure in federal systems, using an unconstitutional federal preemption strategy to crush state resistance, and hiding the entire operation behind a loud, fear-driven story about a "Chinese AI race" that is designed to shut down real scrutiny.